业务简介

第四代英特尔® 至强® 可扩展处理器
安全性

信任您的零信任安全策略

英特尔助您实现严格的安全性、身份、隐私性与合规管理。

全球所有行业的组织都在加速鼓励采用更加安全、可持续的数字化技术，力求实现现代化和激励突破性创新，从而推进业务目标。现代化主要由云、边缘和移动化驱动，许多实际实施的项目需要严格的方式来实现网络安全。实际上，组织面临的网络风险的严重性已成为整个业务风险的核心，成为了董事会层级的问题。

放眼全球，网络安全现已更紧密地融入企业业务目标中，企业建立了零信任安全策略，以确保为重点业务目标而实现的技术足够安全。组织需要更加安全地加速业务洞察和决策智能，因为它们能够优化硬件软件堆栈。

随着组织寻求扩大规模、降低成本和提供新服务，现在比以往任何时候都更需要技术来实现可持续的商业价值。企业无需针对新应用定制系统（这可能会增加复杂性并可能加剧安全漏洞），而是可以通过安全的可扩展平台来实现满足现在和未来各种部署所需的性能。

63% 的组织 **曾受到网络入侵[1]**

37 天和 **240 万美元** **从入侵中恢复平均花费[1]**

88% 的董事会 **认为网络安全是重点业务目标[2]**

运用英特尔技术加速您的安全方案

保护您的业务，助您自信地开展创新。无论业务部署在本地还是云端，保护数据和保持合规都变得愈发重要。配备第四代英特尔® 至强® 可扩展处理器的数据中心拥有经验证的高级安全技术，可在变幻莫测的风险环境中保护数据。同时，即使针对敏感或受监管的数据，也能创造新的商业合作机会和洞察。

借助最新的内置加速器加速 AI、分析、网络、存储和 HPC 等高速增长的工作负载的性能。

关键安全用例

数据保护

在不同行业，无论是制造业（实现数据处理的安全性对于提供精确、高速生产的自动化功能至关重要）还是医疗健康行业（实现数据的安全性对于电子档案保护起到关键作用），您和您客户的数据保护都至关重要。

性能证据点

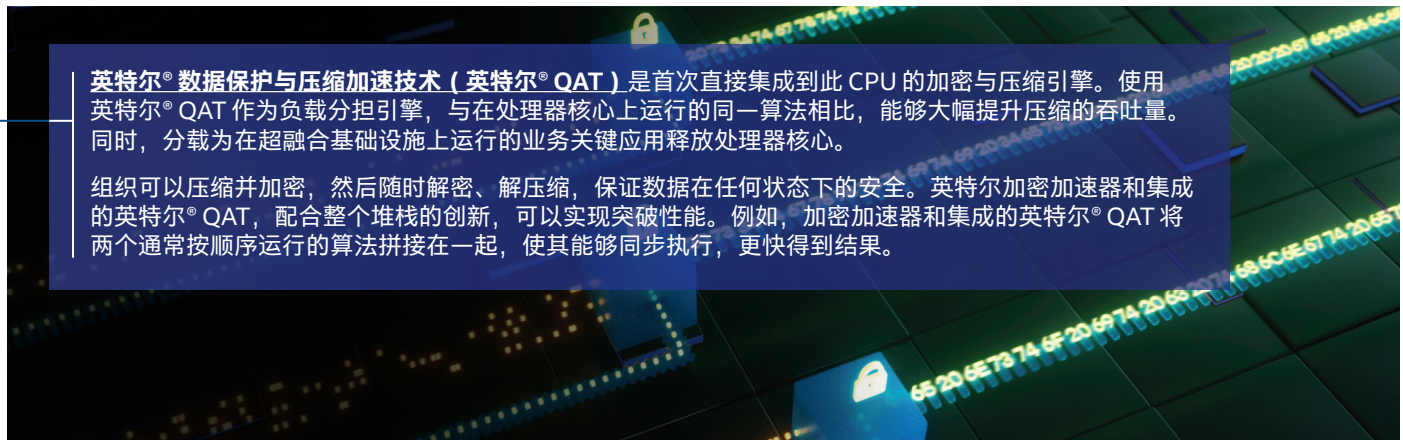
高达 **95%** 的核数减少　和　高达 **2 倍** 的 1 级压缩吞吐量提升

数据基于对使用集成英特尔® QAT 的第四代英特尔® 至强® Platinum 8490H 与前代产品进行比较得出[3]

需求：

随着组织实现现代化，他们需要将计算、网络和存储基础设施整合在一起，连贯、自动且高效地进行部署和管理。在这个一体化基础设施中，数据必须在任何阶段都得到妥善保护（无论是静态、动态或使用中），确保不会丢失关键工作负载的性能。超融合基础设施 (HCI) 通常用于本地或边缘的现代基础设施，作为更大范围的混合云部署的一部分支持广泛的工作负载，包括数据库、分析、企业资源管理 (ERP) 或客户关系管理 (CRM) 软件、虚拟桌面 (VDI) 或工作效率和协作应用。

答案：



英特尔® 数据保护与压缩加速技术（英特尔® QAT）是首次直接集成到此 CPU 的加密与压缩引擎。使用英特尔® QAT 作为负载分担引擎，与在处理器核心上运行的同一算法相比，能够大幅提升压缩的吞吐量。同时，分载为在超融合基础设施上运行的业务关键应用释放处理器核心。

组织可以压缩并加密，然后随时解密、解压缩，保证数据在任何状态下的安全。英特尔加密加速器和集成的英特尔® QAT，配合整个堆栈的创新，可以实现突破性能。例如，加密加速器和集成的英特尔® QAT 将两个通常按顺序运行的算法拼接在一起，使其能够同步执行，更快得到结果。

性能证据点

高达 **2.5 倍** 的吞吐量提升 (RPS)

高达 **74%** 的 P99 延迟减少

高达 **12%** 的 CPU 利用率改善

数据基于对配备两个英特尔® QAT 设备的第四代英特尔® 至强® Platinum 8480+ 处理器与无加速的解决方案进行比较得出[4]

使用机密计算为业务目标提供安全保障

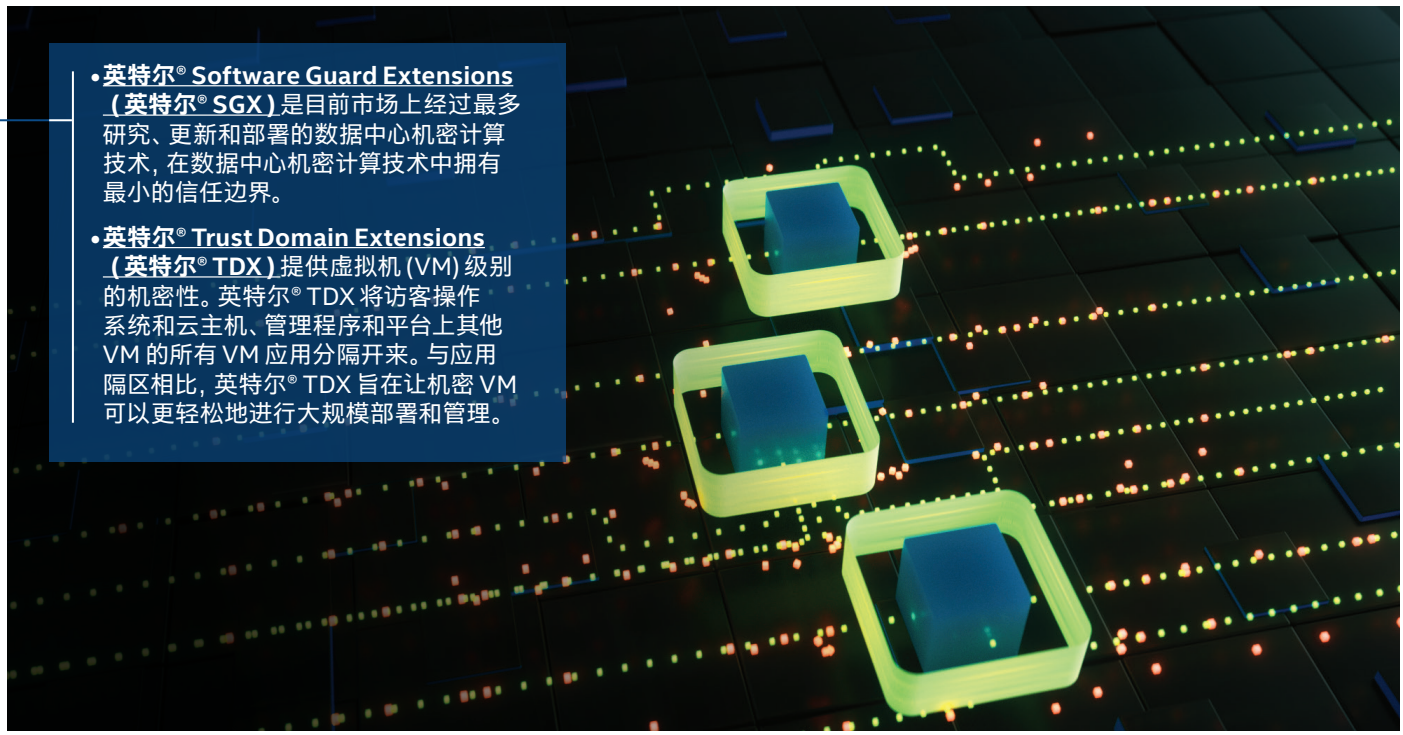
组织十分注重严格的安全性、身份与合规管理，这是他们零信任安全策略的一部分。机密计算可以确保多个业务目标的数据隐私、安全和合规，包括保证政府数据安全或保护金融或银行客户交易数据的安全。

需求：

机密计算通过硬件级内存保护提升敏感数据的独立性。组织需要云共享敏感或受监管的数据，同时让它们在访问受限的隔区内受到更好的保护。数据是推动创新与进步的源动力。企业将数据运用到了方方面面，从检测欺诈到开发响应性更高的供应链，再到训练突破性 AI 模型。因此，加速创新解决方案、自动化流程和提供满意客户体验的步伐，同时建立严格的数据隐私与合规方案，是组织在采用现代化技术时的首要业务目标。

答案：

与静态或动态的传统数据加密不同，机密计算旨在加强使用中的数据的保护与隐私。这些隐私保护至关重要，有助于为分布式网络中具有受监管或其他敏感数据的工作负载提供持续保护，从而利用云的成本、可扩展性和敏捷性优势。在英特尔® SGX 和英特尔® TDX 的加持下，英特尔广泛的机密计算技术产品组合将允许企业选择他们需要的安全级别，以满足自身的业务需求和监管要求。



- **英特尔® Software Guard Extensions（英特尔® SGX）**是目前市场上经过最多研究、更新和部署的数据中心机密计算技术，在数据中心机密计算技术中拥有最小的信任边界。
- **英特尔® Trust Domain Extensions（英特尔® TDX）**提供虚拟机 (VM) 级别的机密性。英特尔® TDX 将访客操作系统和云主机、管理程序和平台上其他 VM 的所有 VM 应用分隔开来。与应用隔区相比，英特尔® TDX 旨在让机密 VM 可以更轻松地进行大规模部署和管理。

此外，**英特尔® Control-Flow Enforcement Technology（英特尔® CET）**也是零信任安全策略的一部分，且能扩展到为隔区外运行的软件提供威胁保护功能。它有助于防止通过控制流劫持攻击（一种恶意软件中最常见的技术）滥用合法代码。

网络管理和网络安全设备

未来工作中新的数字化和自动化经验要求安全、协作和社区环境随时随地在任何设备上都能运行。员工、供应商、合作伙伴和客户需要一个拥有安全、灵活、强大工具的“完整体验”平台，其适应性强且能够高效交付技术与数据，从而帮助他们实现目标。这有助于提升工作的整体幸福感。

需求：

因为需要更安全地远程访问网络和数据，对更强的连接性和更安全技术的需求便应运而生。这些能力让组织可以随时随地安全高效地管理服务，并可随时获取最新报告。部署和管理都变得更加简单，和几乎所有网络连接设备的兼容性可助力实现性能、安全和可扩展性的目标。

性能证据点

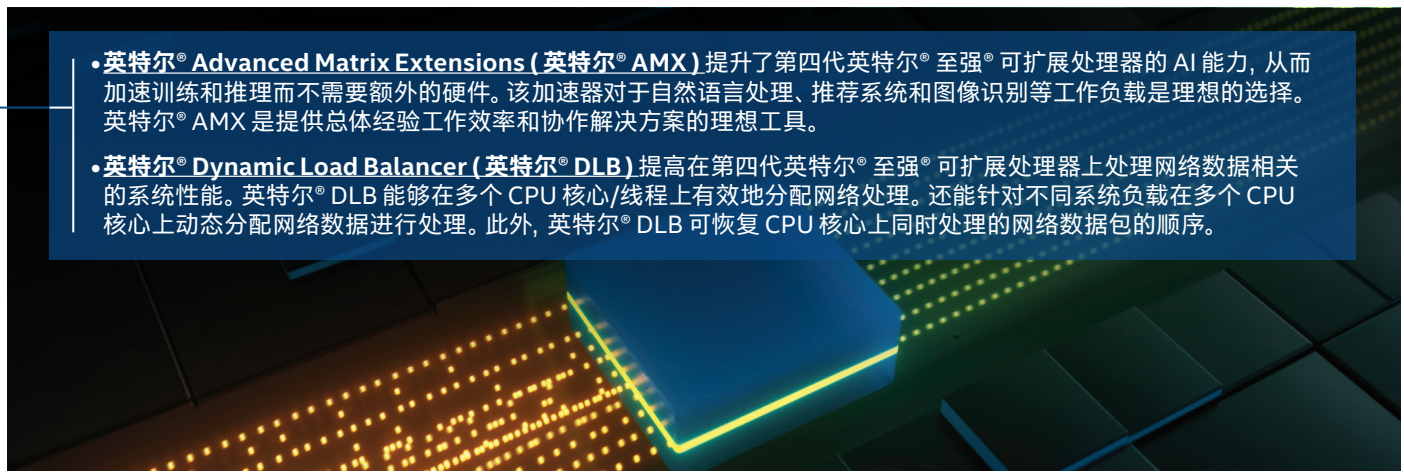
5.7 倍至 10 倍 的 Pytorch 实时推理性能提升[5]

3.5 倍至 10 倍 的 Pytorch 训练性能提升[6]

数据基于对内置的英特尔® AMX (BF16) 与前代产品 (FP32) 进行比较得出

答案：

帮助保护网络安全设备的网络和应用安全性；快速处理加密流量，并采用 AI 驱动的方法进行网络分析、内容检查和恶意软件检测。第四代英特尔® 至强® 可扩展处理器通过新的指令、更快的 DDR5 内存和 PCIe Gen 5 带宽实现高性能和高吞吐量。全新的内置加速器加速 AI、加密和负载平衡，实现性能优化的同时释放 CPU 核心资源。



- **英特尔® Advanced Matrix Extensions（英特尔® AMX）**提升了第四代英特尔® 至强® 可扩展处理器的 AI 能力，从而加速训练和推理而不需要额外的硬件。该加速器对于自然语言处理、推荐系统和图像识别等工作负载是理想的选择。英特尔® AMX 是提供总体经验工作效率和协作解决方案的理想工具。
- **英特尔® Dynamic Load Balancer（英特尔® DLB）**提高在第四代英特尔® 至强® 可扩展处理器上处理网络数据相关的系统性能。英特尔® DLB 能够在多个 CPU 核心/线程上有效地分配网络处理。还能针对不同系统负载在多个 CPU 核心上动态分配网络数据进行处理。此外，英特尔® DLB 可恢复 CPU 核心上同时处理的网络数据包的顺序。

提高工作效率

加入英特尔® 傲腾™ 持久内存，随着数据集增长，以经济实惠的方式增加内存能力，从而以相近的系统成本容纳更多 VM。[7] 要进一步提升网络、存储和计算性能，同时通过将繁重的任务分载到英特尔® Infrastructure Processing Unit（英特尔 IPU）来提高 CPU 利用率。

利用现有基础设施轻松集成

安全技术是零信任安全框架或策略的一部分，为安全文化提供可靠的方案。

英特尔持续创新，在安全的基础上构建，并在数据和基础设施层提供适用于身份、访问和合规管理的安全解决方案。准备好进行部署时，我们可以提供完备的咨询、指导和具体步骤，帮助您快速、可靠地进行现代化。通过英特尔® 合作伙伴联盟，访问 AI、云、高性能计算和其他解决方案领域的专属资源，助您计划、构建并为客户提供更多价值。英特尔拥有广泛的合作伙伴关系、解决方案和体验，通过利用我们全球生态系统中的技术和广泛的合作伙伴关系（CSP、ISV、SI 和原始设备制造商等），英特尔可助您实现安全、可持续的重点业务目标解决方案，将您的愿景和创新变为现实。

支持性统计数字

利用英特尔**超 50,000 个**独特实例类型、规模和区域，获得最多选择。比竞争对手**多 6 倍**。[8]

领导层在数字化转型之旅中的首要业务目标

2022 至 2024 年间，组织领导层（科技和业务公司）在数字化转型方面的投资预计将达到 6.3 万亿美元，到 2024 年，将占所有 IT 支出的 55%。[9] 本业务简介是一系列业务简介的一部分，阐明了领导者在未来的变革中实现业务成功所关注的首要业务目标，以及英特尔硬件、软件和服务（包括第四代英特尔® 至强® 处理器）如何帮助实现这些目标：

- **安全（此简介）：** 实现严格安全性，推动零信任安全策略
- **AI：** 采用数据分析和 AI 推动关键性成果
- **云：** 启动跨混合云、多云与智能边缘的策略
- **重新定义员工体验：** 支持无边界互动式员工体验
- **ESG：** 促进环境中的公平结果与责任 | 社会 | 治理 (ESG)

了解详情

www.intel.cn/xeon/scalable

www.intel.com/security

[1] Accenture，2019 年 11 月 19 日。“AI：为扩展而构建。”https://www.accenture.com/us-en/insights/artificial-intelligence/ai-investments。
[2] 基于英特尔对全球运行 AI 推理工作负载的已安装数据中心服务器进行的市场建模，截至 2021 年 12 月。
[3] 请参阅 [N16]，网址为 intel.com/processorclaims：第四代英特尔® 至强® 可扩展处理器。结果可能会有所不同。
[4] 请参阅 [W5]，网址为 intel.com/processorclaims：第四代英特尔® 至强® 可扩展处理器。结果可能会有所不同。
[5] 请参阅 [A17]，网址为 intel.com/processorclaims：第四代英特尔® 至强® 可扩展处理器。结果可能会有所不同。
[6] 请参阅 [A16]，网址为 intel.com/processorclaims：第四代英特尔® 至强® 可扩展处理器。结果可能会有所不同。
[7] 第三代英特尔® 至强® 可扩展处理器与 AMD EPYC 相比。请参阅配置详情 [126-130]，网址为 www.intel.com/3gen-xeon-config。
[8] 来源：Liftr Insights 历史组件跟踪数据 + 英特尔内部初步分析，截至 2022 年 9 月 2 日。
[9] IDC，2021 年 10 月。“IDC FutureScape：2022 年全球数字化转型预测。”https://www.idc.com/getdoc.jsp?containerId=US47115521。

1122/MH/MESH/350497-002US